



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/656,315	09/06/2000	KIL-HO SHIN	107215	9436
25944	7590	11/05/2004	EXAMINER	
OLIFF & BERRIDGE, PLC P.O. BOX 19928 ALEXANDRIA, VA 22320			LAFORGIA, CHRISTIAN A	
			ART UNIT	PAPER NUMBER
			2131	
DATE MAILED: 11/05/2004				

5

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/656,315	Applicant(s) SHIN ET AL.
	Examiner Christian La Forgia	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 18 March 2002.

2a) This action is **FINAL**. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 1-52 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 1-52 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 23 October 2000 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
5) Notice of Informal Patent Application (PTO-152)
6) Other: _____.

37 CFR 1.105 Requirement

1. Applicant and the assignee of this application are required under 37 CFR 1.105 to provide the following information that the examiner has determined is reasonably necessary to the examination of this application.
2. In response to this requirement, please provide copies of each patent or patent application, including foreign patents and foreign patent applications along with a translation that names any one of the inventors of the instant application.
3. The applicant is reminded that the reply to this requirement must be made with candor and good faith under 37 CFR 1.56. Where the applicant does not have or cannot readily obtain an item of required information, a statement that the item is unknown or cannot be readily obtained will be accepted as a complete reply to the requirement for that item.
4. This requirement is an attachment of the enclosed Office action. A complete reply to the enclosed Office action must include a complete reply to this requirement. The time period for reply to this requirement coincides with the time period for reply to the enclosed Office action.

DETAILED ACTION

5. Claims 1-52 have been presented for examination.

Drawings

6. The drawings were received on 23 October 2000. These drawings are acceptable.

Specification

7. The incorporation of essential material in the specification by reference to a foreign application or patent, or to a publication is improper. Applicant is required to amend the disclosure to include the material incorporated by reference. The amendment must be

accompanied by an affidavit or declaration executed by the applicant, or a practitioner representing the applicant, stating that the amendatory material consists of the same material incorporated by reference in the referencing application. See *In re Hawkins*, 486 F.2d 569, 179 USPQ 157 (CCPA 1973); *In re Hawkins*, 486 F.2d 579, 179 USPQ 163 (CCPA 1973); and *In re Hawkins*, 486 F.2d 577, 179 USPQ 167 (CCPA 1973).

8. A substitute specification in proper idiomatic English and in compliance with 37 CFR 1.52(a) and (b) is required. The substitute specification filed must be accompanied by a statement that it contains no new matter.

Claim Rejections - 35 USC § 112

9. The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

10. Claims 43-45 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The Examiner could not find means for derandomizing information. This rejection can be overcome by referring to the text of the Specification that provides a teaching of derandomizing.

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Regarding claims 3 and 7, the phrase "such as" renders the claim indefinite because it is unclear whether the limitations following the phrase are part of the claimed invention. See MPEP § 2173.05(d).

13. Claims 14-37 and 46 recite the limitation "the fourth storage means" and "the fifth storage means" throughout the claim language. There is insufficient antecedent basis for this limitation in the claim.

14. Claims 43-45 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Where applicant acts as his or her own lexicographer to specifically define a term of a claim, the written description must clearly define the claim term and set forth the uncommon definition so as to put one reasonably skilled in the art on notice that the applicant intended to so define that claim term. See MPEP § 608.01(o). See *Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1357, 52 USPQ2d 1029, 1033 (Fed. Cir. 1999). The term "derandomizing" is undefined according to the dictionaries and other resources available to the Examiner. Further, the Applicant fails to meet the requirements of redefining a term as set forth in the MPEP § 2106. In order to define/redefine a term, the Applicant must do so "with reasonable clarity, deliberateness, and precision" and must "set out his uncommon definition in some manner within the patent disclosure' so as to give one of ordinary skill in the art notice of the change" in meaning. The Applicant fails to clearly, deliberately and precisely define the term derandomizing.

Claim Rejections - 35 USC § 102

15. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

16. Claims 1-52 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 5,987,134 to Shin et al., hereinafter Shin

17. The applied reference has a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention “by another,” or by an appropriate showing under 37 CFR 1.131.

18. As per claims 1 and 47, Shin discloses a data storage device provided with a function for authenticating a user's access right, which verifies legitimacy of proof data generated for proving a right of an application program to access data stored in a storage medium, to thereby authenticate the access right of a user of the application program to the data, the data storage device comprising:

first storage means for storing authentication data (column 2, lines 37-55, i.e. “To achieve the objects and in accordance with the purpose of the invention, as embodied and broadly

described herein, one aspect of a device for authenticating user's access rights to resources of the present invention comprises first memory means for storing challenging data");

second storage means for storing user unique identifying information of the user of the application program (column 2, lines 42-55, i.e. "second memory means for storing unique identifying information of the user");

third storage means for storing auxiliary proof information being a result in which a specific calculation is executed to the user unique identifying information of the application program and unique security characteristic information (column 2, lines 43-55, i.e. "third memory means for storing proof support information which is a result of executing predetermined computations to the user unique identifying information and unique security characteristic information of the device");

proof data generation means for executing a specific calculation to the authentication data stored in the first storage means, the user unique identifying information of the application program stored in the second storage means, and the auxiliary proof information stored in the third storage means, to thereby generate proof data (column 2, lines 47-55, i.e. "response generation means for generating a response from the challenging data stored in the first memory means, the unique identifying information stored in the second memory means and the proof support information stored in the third memory means, and verification means for verifying the legitimacy of the response by verifying that the response, the challenging data and the unique security characteristic information of the device satisfy a specific predefined relation");

a data storage main frame provided with a storage medium, which stores and preserves data in the storage medium (column 1, lines 37-43, column 5, line 65 to column 6, line 4, i.e.

“The user mounts personal computer/workstation using a designated method. When the user starts up the application program and when the execution of the program reaches the user authentication routine, the program communicates with the hardware in which the authentication key of the user is embedded.” Shin discloses an application program, which must be stored on some type of storage medium in order to execute.);

command generation means installed in the application program, for generating a command that instructs an operation to the data stored in the storage medium of the data storage main frame (column 6, lines 5-15; i.e. “the verification routine **15** is set to the application program”);

command issuing means installed in the application program, for issuing the command generated by the command generation means to the outside of the application program (column 6, lines 5-15, i.e. “The verification routine **15** is same as that of the conventional technologies in that it communicates with the response generation program **17** retained by the user”);

proof data verification means for verifying that the proof data generated by the proof data generation means has been generated on the basis of the unique security characteristic information (column 6, lines 16-28, i.e. “Data to be transferred (challenging data **18**) and expected returned data (expected value) are embedded in the verification routine **15**. The verification routine **15** fetches the data to be transferred and transfers it to the user, and receives the returned data from the user. Then the verification routine **15** compares the returned data from the user with the expected value: if they are identical with each other, the verification routine **15** executes the next step of the program; if they are not identical, the verification routine **15** halts the execution of the program”); and

command management means for permitting to execute the command only when the verification is successful, as to at least one type of the command that instructs the operation to the data stored in the data storage main frame (column 6, lines 16-28, i.e. "Data to be transferred (challenging data 18) and expected returned data (expected value) are embedded in the verification routine 15. The verification routine 15 fetches the data to be transferred and transfers it to the user, and receives the returned data from the user. Then the verification routine 15 compares the returned data from the user with the expected value: if they are identical with each other, the verification routine 15 executes the next step of the program; if they are not identical, the verification routine 15 halts the execution of the program").

19. Regarding claims 2, 6, 22, 25, 30, 34, and 37, Shin discloses wherein at least the second storage means and the proof data generation means are retained in protection means for making it difficult to observe the inner data and processing procedures from the outside (column 3, lines 9-15, claim 2).

20. Regarding claims 3 and 7, Shin discloses wherein at least the second storage means and the proof data generation means are configured in a small portable processor such as an IC card (column 3, lines 9-15, claim 3).

21. Regarding claim 4, Shin discloses wherein the proof data generation means includes first calculation means and second calculation means, in which the first calculation means executes a specific calculation to the user unique identifying information of the application program stored

in the second storage means and the auxiliary proof information stored in the third storage means to produce the unique security characteristic information as a result of the calculation, and the second calculation means executes a specific calculation to the authentication data stored in the first storage means and the unique security characteristic information calculated by the first calculation means to generate the proof data as a result of the calculation (column 3, lines 16-28; claim 4).

22. Regarding claim 5, Shin discloses wherein the proof data generation means includes third calculation means, fourth calculation means, and fifth calculation means, in which the third calculation means executes a specific calculation to the authentication data stored in the first storage means and the auxiliary proof information stored in the third storage means, the fourth calculation means executes a specific calculation to the authentication data stored in the first storage means and the user unique identifying information of the application program stored in the second storage means, and the fifth calculation means executes a specific calculation to a calculation result by the third calculation means and a calculation result by the fourth calculation means, to generate the proof data as a result of the calculation (column 3, lines 29-47; claim 5).

23. Regarding claim 8, Shin discloses wherein the unique security characteristic information is a decryption key in an encryption function, the authentication data is appropriate data encrypted by using an encryption key corresponding to the decryption key, and the proof data verification means verifies that the proof data generated by the proof data generation means is identical to the correct decryption of the authentication data (claim 8).

24. Regarding claim 9, Shin discloses wherein the unique security characteristic information is an encryption key in an encryption function, and the proof data generated by the proof data generation means is verified to be the authentication data correctly encrypted by using the encryption key (claim 9).

25. Regarding claim 10, Shin discloses wherein the unique security characteristic information is a signature key in a digital signature function, and the proof data generated by the proof data generation means is verified to be a digital signature to the authentication data generated by using the signature key (claim 10).

26. With regards to claims 11 and 39, Shin teaches wherein the encryption function is an asymmetric encryption function, and the unique security characteristic information is a key on one side (claims 11 and 12).

27. Concerning claims 12 and 40, Shin teaches wherein the encryption function is a public key encryption function, and the unique security characteristic information is a private key (claims 13 and 14).

28. With regards to claims 13 and 41, Shin discloses wherein the encryption function is a symmetric encryption function, and the unique security characteristic information is a common secret key (claims 15 and 16).

29. Regarding claim 14, Shin discloses wherein the proof data verification device writes the authentication data stored in the fourth storage means into the first storage means of the proof data generation device, the proof data generation device writes the proof data generated on the basis of the authentication data written into the first storage means by the proof data generation means into the fifth storage means of the proof data verification device, and the proof data verification device authenticates the user's access right by using the proof data written into the fifth storage means (claim 17).

30. With regards to claim 15, Shin teaches wherein the unique security characteristic information is an encryption key in an encryption function, the proof data verification device includes random number generation means, the random number generation means writes a random generated number into the fourth storage means as the authentication data, and the proof data verification means verifies the proof data written into the fifth storage means by the proof data generation device to be the encryption of the random number being the authentication data using encryption key being the unique security characteristic information (claim 18).

31. With regards to claim 16, Shin discloses wherein the unique security characteristic information is a decryption key in an encryption function, the proof data verification device includes random number generation means, sixth storage means for storing a generated random number, and seventh storage means for storing a seed for authentication data, the random number generation means writes a generated random number into the sixth storage means, randomizes

the seed for authentication data stored in the seventh storage means by using the random number, and thereafter writes the result of the randomization as the authentication data into the fourth storage means, and the proof data verification means verifies the result with the random number effect by the random number stored in the sixth storage means removed from the proof data written into the fifth storage means to be identical to the decryption of the seed for authentication data stored in the seventh storage means by the decryption key being the unique security characteristic information (claim 19).

32. With regards to claim 17, Shin teaches wherein the unique security characteristic information is a signature key in a digital signature function, the proof data verification device includes random number generation means, the random number generation means writes a generated random number into the fourth storage means as the authentication data, and the proof data verification means verifies the proof data written into the fifth storage means by the proof data generation device to be a digital signature to the authentication data being the random number by the signature key being the unique security characteristic information (claim 20).

33. Concerning claim 18, Shin teaches wherein the encryption function is of the RSA public key crypto-system using a modulus n, the unique security characteristic information is a private key D, a public key corresponding to the private key D is E, and the proof data verification means verifies E power of proof data R written into the fifth storage means to be congruent with an authentication data C stored in the fourth storage means, modulo n ($R^E \bmod n = C \bmod n$) (column 8, line 3 to column 10, line 35, claim 21).

34. Concerning claim 19, Shin discloses wherein the encryption function is of the RSA public key crypto-system using a modulus n, the unique security characteristic information is a private key D, a public key corresponding to the private key D is E, the seed for authentication data stored in the seventh storage means is a number K' being E power of a data K modulo n ($K' = K^E \bmod n$), the random number generation means writes a number C being E power of a random number r modulo n multiplied by the number K' modulo n ($C = r^E K' \bmod n$) into the fourth storage means as the authentication data, and the proof data verification means verifies a reverse modulo n of the random number r stored in the sixth storage means multiplied by proof data R written into the fifth storage means to be congruent with the data K modulo n ($K \bmod n = r^{-1} R \bmod n$) (column 10, line 38 to column 14, line 18; claim 22).

35. Concerning claim 20, Shin discloses wherein the encryption function is of the RSA public key crypto-system using a modulus n, the unique security characteristic information is the private key D, the public key corresponding to the private key D is E, auxiliary proof information t stored in the third storage means is data obtained by subtracting user unique identifying information e of the application program stored in the second storage means from the private key D, and adding a product of a value of a non-collision function ω ($= G(n, e)$) dependent on the modulus n and the user unique identifying information e, and an Eulerian number $\Phi(n)$ ($t = D - e + \omega\Phi(n)$), and the proof data generation means generates the proof data by calculating D power of C modulo n ($C^D \bmod n$), from the t, the e, and the authentication data C stored in the first storage means (column 14, line 22 to column 15, line 52, claims 23 and 24).

36. Concerning claim 21, Shin teaches wherein the proof data generation means includes third calculation means, fourth calculation means, and fifth calculation means, the third calculation means calculates the t power of the C modulo n ($C^t \bmod n$), the fourth calculation means calculates the a power of the C modulo n ($C^a \bmod n$), and the fifth calculation means multiplies a result of the calculation by the first calculation means by that of the calculation by the second calculation means modulo n to thereby generate the proof data R ($=C^t C^a \bmod n$) (claims 25 and 26).

37. Concerning claim 23, Shin discloses wherein the encryption function is of the RSA public key crypto-system using a modulus n ., the unique security characteristic information is the private key D , the public key corresponding to the private key D is E , auxiliary proof information t stored in the third storage means is data obtained by adding to the D a value of a non-collision function $F(n, e)$ which is dependent on the modulus n and user unique identifying information a of the application program stored in the second storage means ($t = D + F(n, e)$), and the proof data generation means generates the proof data by calculating D power of C modulo n ($C^D \bmod n$), from the t , the e , and the authentication data C stored in the first storage means (claims 29 and 30).

38. Concerning claims 24 and 29, Shin discloses wherein the proof data generation means includes third calculation means, fourth calculation means, and fifth calculation means, the third calculation means calculates the t power of the C modulo n ($C^t \bmod n$), the fourth calculation

means calculates the $F(n, e)$ power of the C modulo n ($C^{F(n,e)} \bmod n$), and the fifth calculation means multiplies a result of the calculation by the third calculation means by the reverse of a calculation result by the fourth calculation means modulo n to thereby generate the proof data R ($=C^t C^{F(n,e)} \bmod n$) (claims 31 and 32).

39. Concerning claim 26, Shin discloses wherein the encryption function is of the Pohlig-Hellman asymmetric crypto-system using a modulus p , the unique security characteristic information is a key D on one side, a key on the other side corresponding to the key D is E ($DE \bmod p-1 = 1$), and the proof data verification means verifies E power of proof data R written into the fifth storage means to be congruent with authentication data C stored in the fourth storage means, modulo p ($R^E \bmod p = C \bmod p$) (column 18, line 13 to column 19, line 67, claim 35).

40. Concerning claim 27, Shin teaches wherein the encryption function is of the Pohlig-Hellman asymmetric crypto-system using a modulus p , the unique security characteristic information is a key D on one side, a key on the other side corresponding to the key D is E ($DE \bmod p-1 = 1$), the seed for authentication data stored in the seventh storage means is a number K' being E power of a data K modulo p ($K' = K^E \bmod p$), the random number generation means writes a number C that is identical to E power of a random number r modulo p multiplied by the number K' modulo p ($C = r^E K' \bmod p$) into the fourth storage means as the authentication data, and the proof data verification means verifies a reverse modulo p of the random number r stored in the sixth storage means multiplied by the proof data R written into the fifth storage means to

be congruent with the data K modulo p ($K \bmod p = r^{-1}R \bmod p$) (column 18, line 13 to column 19, line 67, claim 36).

41. Concerning claim 28, Shin discloses wherein the encryption function is of the Pohlig-Hellman asymmetric crypto-system using a modulus p, the unique security characteristic information is a key D on one side, a key on the other side corresponding to the key D is E ($DE \bmod p-1 = 1$), auxiliary proof information t stored in the third storage means is data obtained by adding to the D a value of a non-collision function $F(p, e)$ which is dependent on the modulus p and user unique identifying information a of the application program stored in the second storage means ($t = D + F(p, e)$), and the proof data generation means generates the proof data by calculating D power of C modulo p ($C^D \bmod p$), from the t, the e, and the authentication data C stored in the first storage means (column 18, line 13 to column 19, line 67, claims 37 and 38).

42. Concerning claim 31, Shin discloses wherein the encryption function is of the ElGamal public key crypto-system using a modulus p of the ElGamal public key crypto-system using a modulus p and a generator a, the unique security characteristic information is a private key X, a public key corresponding to the key X is Y ($Y = a^x \bmod p$), a is a number that the a is exponentiated by an appropriate random number z as an exponent modulo p ($u = a^z \bmod p$), and K' is a product of data K and the Y exponentiated by the random number z modulo p ($K' = Y^z K \bmod p$), a combination of the a and the K' is stored in the seventh storage means as the seed for authentication data, the random number generation means writes the « and a number C that results from a random number r multiplied by the number K' modulo p ($C = rK' \bmod p$) into the

fourth storage means as the authentication data, and the proof data verification means verifies a reverse modulo p of the random number r stored in the sixth storage means multiplied by proof data R written into the fifth storage means to be congruent with the data K modulo p ($K \bmod p = r^{-1}R \bmod p$) (column 20, line 2 to column 22, line 17, claim 43).

43. Concerning claim 32, Shin discloses wherein, when the encryption function is of the ElGamal public key crypto-system using a modulus p and a generator a, the unique security characteristic information is a key X on one side, a public key corresponding to the key X is Y ($Y = a^x \bmod p$), auxiliary proof information t stored in the third storage means is data obtained by adding to the X a value of a non-collision function $F(p, e)$ which is dependent on the modulus p and user unique identifying information a of the application program stored in the second storage means ($t = X + F(p, e)$), and the proof data generation means generates the proof data by calculating C divided by X^e modulo p ($Cu^{-X} \bmod p$), from the t, the e, and the authentication data a and C stored in the first storage means (column 20, line 2 to column 22, line 17, claim 44).

44. Concerning claim 33, Shin discloses wherein the proof data generation means includes third calculation means, fourth calculation means, and fifth calculation means, the third calculation means calculates the t power of the a modulo p ($u^t \bmod p$), the fourth calculation means calculates the $F(p, e)$ power of the a modulo p ($u^{F(p, e)} \bmod p$), and the fifth calculation means divides the C by a calculation result of the third calculation means modulo p and

multiplies a calculation result of the fourth calculation means to thereby generate the proof data $R (= Cu^{-1} u^{F(p,e)} \bmod p)$ (claim 45).

45. Concerning claim 35, Shin discloses wherein the digital signature function is of the ElGamal signature scheme using the modulus p and a generator a , the unique security characteristic information is a signature key X , a public key corresponding to the key X is Y ($Y = a^x \bmod p$), and the proof data verification means verifies, in regard to a proof data R and S , a value being the a exponentiated by authentication data C as an exponent stored in the fourth storage means, modulo p to be congruent with a product of the R power of the Y and the S power of the R , modulo p ($a^c \bmod p = Y^R R^S \bmod p$) (claim 47).

46. Concerning claim 36, Shin discloses wherein the digital signature function is the ElGamal signature under the modulus p and a generator a , the unique security characteristic information is the signature key X , the public key corresponding to the key X is Y ($Y = a^x \bmod p$), auxiliary proof information t stored in the third storage means is data obtained by adding to the X a value of a non-collision function $F(p,e)$ which is dependent on the modulus p and a user unique identifying information a of the application program stored in the second storage means ($t = X + F(p,e)$), and the proof data generation means generates an appropriate random number k in generating the proof data R and S , adopts the k power of the a modulo p as the R ($= a^k \bmod p$), subtracts a product of the X and the R from the C modulo $p-1$ and multiplies the calculation result with a reverse of the k , from the t , the e , and the authentication data C written into the first storage means, and thereby calculates the S ($= (C-RX)k^{-1} \bmod p-1$) (claim 48).

47. With regards to claim 38, Shin discloses wherein the user unique identifying information of the application program is a decryption key of an encryption function, the auxiliary proof information is the unique security characteristic information encrypted by an encryption key corresponding to the decryption key, and the first calculation means decrypts the auxiliary proof information by using the decryption key being the user unique identifying information of the application program to thereby calculate the unique security characteristic information (claim 50).

48. With regards to claim 42, Shin discloses wherein the proof data verification means includes eighth storage means for storing clear text data corresponding to the authentication data or the seed for authentication data being encrypted data and comparison means, and the comparison means compares the proof data generated by the proof data generation means or a result having the random number effect removed from the proof data with the clear text data stored in the eighth storage means, and only when both are identical, judges the proof data to be legitimate (claims 54 and 55).

49. With regards to claim 43, Shin discloses wherein the proof data verification means includes ninth storage means for storing a result having a specific one-way function applied to clear text data corresponding to the authentication data or the seed for authentication data being encrypted data, sixth calculation means, and comparison means, the sixth calculation means applies the one-way function to the proof data generated by the proof data generation means after

derandomizing if necessary, and the comparison means compares a calculation result by the sixth calculation means with data stored in the ninth storage means, and only when both are identical, judges the proof data to be legitimate (claims 56 and 57).

50. With regards to claim 44, Shin discloses wherein the proof data verification means includes program execution means, the authentication data or the seed for authentication data is data obtained by encrypting a program, the proof data verification means passes, after derandomizing if necessary, the proof data generated by the proof data generation means to the program execution means as a program, whereby the program execution means executes a correct operation, when the proof data generation means correctly decrypts the authentication data or the seed for authentication data being an encrypted program, namely, only when the encrypted program is correctly decrypted (claim 58).

51. With regards to claim 45, Shin discloses wherein the proof data verification means includes program execution means, program storage means, and program decryption means, a program stored in the program storage means is encrypted to a part or whole thereof, the authentication data or the seed for authentication data is data obtained by separately encrypting a decryption key for decrypting the encrypted program, the proof data verification means passes the proof data generated by the proof data generation means to the program decryption means, the program decryption means uses, after derandomizing if necessary, the proof data generated by the proof data generation means as a decryption key to thereby decrypt a necessary part of the program stored in the program storage means, the program execution means executes the

decrypted program, whereby, when the proof data generation means correctly decrypts the authentication data or the seed for authentication data, namely, only when the decryption key for decrypting the encrypted program is correctly decrypted, the program execution means executes a correct operation (claim 59).

52. Concerning claim 46, Shin teaches wherein the proof data generation device and the proof data verification device are installed in one enclosure, and the proof data generation device and the proof data verification device communicate with each other without using a communication medium outside the enclosure (claim 62).

53. Regarding claim 48, Shin discloses wherein the storage medium of the data storage device is a write once optical storage medium (column 9, lines 29-38).

54. With regards to claim 49, Shin teaches wherein the write once optical storage medium of the data storage device is a phase change type optical storage medium (column 9, lines 29-38).

55. With regards to claim 50, Shin discloses wherein the write once optical storage medium of the data storage device is a phase separation type optical storage medium (column 9, lines 29-38).

56. Regarding claim 51, Shin discloses wherein the storage medium that first stores at least a specific access log, of the storage medium of the data storage device, is a write once optical storage medium (column 9, lines 29-38).

57. As per claim 52, Shin discloses a data storage device, comprising a write once optical storage medium that is used for a part that first stores a specific access log as auxiliary storage means (column 9, lines 29-38).

Conclusion

58. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

59. The following patents are cited to further show the state of the art with respect to authenticating user's access rights, such as:

United States Patent No. 6,516,413 to Aratani et al., which is cited to show user authentication.

United States Patent No. 6,615,352 to Terao et al., which is cited to show authenticating user's access rights to resources.

United States Patent No. 6,718,470 to Adams, which is cited to show granting security privilege in a communications system.

United States Patent No. 6,088,802 to Bialick et al., which is cited to show peripheral device with integrated security functionality.

United States Patent No. 6,108,420 to Larose et al., which is cited to show installation of uniquely customized, authenticable, and traceable software application.

United States Patent No. 6,185,681 to Zizzi, which is cited to show transparent encryption and decryption for an electronic document management system.

United States Patent No. 6,567,915 to Guthery, which is cited to show IC card with identity authentication table and authorization tables defining access rights.

60. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

61. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

62. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131

clf


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100